HN

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/025,541	12/26/2001	Robert Edward Moore	01.133.01	8301

7590 01/20/2006

Zilka-Kotab, PC
P.O. Box 721120
San Jose, CA 95172-1120

EXAMINER
BLUDAU, BRANDON S

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 01/20/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/025,541	**Applicant(s)** MOORE ET AL.
	Examiner Brandon S. Bludau	**Art Unit** 2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 October 2005*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,4-11,14-21 and 24-35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1, 4-5, 8-11, 14-15, 18-21, 24-25, 28-32, 34* is/are rejected.

7)☒ Claim(s) *6,7,16,17,26,27,33 and 35* is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) □ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) □ Notice of Informal Patent Application (PTO-152)
6) □ Other: _____.

DETAILED ACTION

This action is responsive to communications: application, filed 12/26/2001; amendment filed 10/13/2005.

Claims 1, 4-11, 14-21 and 24-35 are pending in the case. Claims 2,3,12,13,22 and 23 are cancelled. Claims 31-35 are added. Claims 1, 11 and 21 are independent claims.

Response to Arguments

Applicant's arguments filed 10/13/2005 regarding "target words" have been fully considered but they are not persuasive. In regards to the independent claims 1, 11, and 21, the Applicant argues the Examiner's use of Kuo in the rejection of "searching code operable to search within said computer file for text data containing one or more target words that match at least one of a word or a characteristic of a word within a predetermined word library". The Applicant does not believe that the reference's teaching of "sequences of computer-readable characters that portray viruses ... or a series of characters found within, known viruses" meets the limitation of "target words" as disclosed by the Applicant. The examiner points out definitions found in the American Heritage College Dictionary 4th edition. *Word*: "A combination of sounds ... or its representation in writing, that symbolizes and communicates a meaning." *Character*: "one of a set of symbols, such as letters or numbers, that are arranged to express information." The examiner points out that a word is inherently a series of characters arranged to express information. Therefore a series of characters, as found in Kuo, portraying a virus or representing sequences that are known to be found within viruses, are necessarily words that communicate a meaning and express information and thus cover the Applicant's claimed "target words".

Applicant's arguments filed 10/13/2005, with respect to the rejection(s) of claim(s) 1,11, 21 regarding context identifying code have been fully considered but are rendered moot based on the changed scope of the now amended claims. Therefore, a new rejection on the amended claim is made in view of Chen (US Patent 5960170).

Applicant's arguments filed 10/13/2005, with respect to the rejection(s) of claim(s) 6,7 et al. regarding adjusting trigger thresholds to be more sensitive have been fully considered and are persuasive. Therefore, the rejections have been withdrawn.

Applicant's arguments filed 10/13/2005, with respect to the rejection(s) of claim(s) 9 et al. regarding the portions of a computer file being searched are rendered moot based on the changed scope of the now amended independent claims. Therefore, a new rejection on the amended claim is made in view of Chen (US Patent 5960170).

Claim Rejections - 35 USC § 103

1. Claims 1,4-5,8-11,14-15,18-21,24-25,28-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kuo (US Patent 6230288) and further in view of Chen (US Patent 5960170).

2. As per claim 1, Kuo discloses a computer program product embodied on a computer readable medium operable for controlling a computer to identify a computer file as potentially containing malware, said computer program comprising:

Searching code operable to search within said computer file for text data containing one or more target words that match at least one of a word or a characteristic of a word within a predetermined word library (column 4 lines 15-27);

wherein said predetermined word library includes one or more of:

Words that are names associated with known malware authors (column 4 lines 15-27; A name by definition is "a word or words by which an entity is designated and distinguished from others," therefore it is consistent with a virus signature, as a signature is a characteristic indicating identity);

Word format characteristics that are indicative of words being part of a message embedded within said computer file by a malware author; and

Word suffix characteristics that are indicative of words being part of a message embedded within said computer file by a malware author. (The examiner rejects these limitations on the basis that they are all consistent with the characteristics of virus signatures.)

Kuo does not disclose:

Context identifying code operable to identify a context within said computer file of said one or more target words; and

File identifying code operable if said context matches one or a predetermined set of contexts to identify said computer file as potentially containing malware;

wherein said predetermined sets of contexts includes one or more of:

Within a script portion of a webpage;

Within a comment of a webpage;

Within a predetermined proximity to another target word.

Chen does disclose:

Context identifying code operable to identify a context within said computer file of said one or more target words (column 13 line 57 – column 14 line 38); and

File identifying code operable if said context matches one or a predetermined set of contexts to identify said computer file as potentially containing malware (column 13 line 57 – column 14 line 38);

wherein said predetermined sets of contexts includes one or more of:

Within a script portion of a webpage;

Within a comment of a webpage;

Within a predetermined proximity to another target word (column 14 lines 16-38).

Chen is analogous art because it is directed towards a method of virus detection.

It would have been obvious for one of ordinary skill in the art at the time of the invention to modify Kuo to include context identifying code wherein the virus detection method could determine if target words are found within a predetermined proximity to another word.

Motivation for one to modify Kuo as discussed above would have been to enable the virus scan to selectively and iteratively search for virus signatures thus effectively reducing processing needs and data transmissions as implied in Chen column 14.

3. As per claim 4, Kuo discloses a computer program product as claimed in claim 1, wherein, if said computer file is identified as potentially containing malware, then malware found code triggers one or more malware found action (column 7 lines 36-38).

4. As per claim 5, Kuo discloses a computer program product as claimed in claim 4, wherein said malware found actions include one or more of:

Quarantining said computer file;

Deleting said computer file;

Issuing a warning message concerning said computer file (column 7 lines 36 – 38); and

Deleting a portion of said computer file suspect of containing malware.

5. As per claim 8, Kuo discloses a computer program product as claimed in claim 1, wherein all of said computer file is searched for said target words (column 4 lines 53-55).

6. As per claim 9, Kuo discloses a computer program product as claimed in claim 1, but does not disclose wherein only those portions of said computer file matching said predetermined set of contexts are searched for said target words.

Chen does disclose wherein only those portions of said computer file matching said predetermined set of contexts are searched for said target words (column 13 line 57 – column 14 line 38 wherein the predetermined context is within proximity to another target word).

Chen is analogous art because it is directed towards a method for virus detection.

It would have been obvious for one of ordinary skill in the art at the time of the invention to modify Kuo to include only searching those portions of the file that contain the predetermined context in this case the proximity to another word.

Motivation for one to modify Kuo as discussed above would have been to enable the virus scan to selectively and iteratively search for virus signatures thus effectively reducing processing needs and data transmissions as implied in Chen column 14.

7. As per claim 10, Kuo discloses a computer program product as claimed in claim 1, wherein said malware comprises one or more of a computer virus, a worm and a Trojan. (column 4 lines 22 – 25).

8. Claim 11 is rejected because it discloses the same matter as claim 1.

9. Claim 14 is rejected because it discloses the same matter as claim 4.

10. Claim 15 is rejected because it discloses the same matter as claim 5.

11. Claim 18 is rejected because it discloses the same matter as claim 8.

12. Claim 19 is rejected because it discloses the same matter as claim 9.

13. Claim 20 is rejected because it discloses the same matter as claim 10.

14. Claim 21 is rejected because it discloses the same matter as claim 1.

15. Claim 24 is rejected because it discloses the same matter as claim 4.

16. Claim 25 is rejected because it discloses the same matter as claim 5.

17. Claim 28 is rejected because it discloses the same matter as claim 8.

18. Claim 29 is rejected because it discloses the same matter as claim 9.

19. Claim 30 is rejected because it discloses the same matter as claim 10.

20. As per claim 31, Kuo discloses a computer program product as claimed in claim 1, wherein said predetermined word library includes: words that are names associated with known malware authors; words that are indicative of being part of a message embedded within said computer file by a malware author; word format characteristics

that are indicative of words being part of a message embedded within said computer file by a malware author; and word suffix characteristics that are indicative of words being part of a message embedded within said computer file by a malware author (the examiner rejects all of these with Kuo column 4 lines 15-27 under the basis that virus signatures contain all of these characteristics by definition, in that words or names indicative of being part of a malware author's message makes up the virus signatures).

21. As per claim 32, Kuo and Chen disclose a computer program product as claimed in claim 1, wherein said predetermined set of contexts includes: within a predetermined proximity to another target word (Chen column 14 lines 16-38); and within executable code (Chen column 19 lines 4-14 wherein the executable code is inherently present in the executable object); but do not disclose wherein the set includes within a script portion of a webpage; within a comment of a webpage.

However, it is a well-known method at the time of the invention in the art of virus scanning to implement Internet gateway scanners that scan all traffic before entering a network. A common practice of gateway scanners is to inspect the html content of web pages including scripts, headers, applets and comments so as to prevent malicious content from entering the network. Therefore it would have been well known in the art at the time of the invention to include the scanning of script and comments of webpages for malware content.

Motivation for one to modify Kuo and Chen as discussed above would have been to prevent the entering of malicious content on a computer through the access of webpages from the internet as would be well known in the art and as is applied to well known gateway scanners.

22. Claim 34 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kuo (US Patent 6230288) in view of Chen (US Patent 5960170) and further in view of Rubin (Trend InterScan Secures Top Virus-Protection Spot).

As per claim 34, Kuo and Chen disclose a computer program product as claimed in claim 1, but do not disclose wherein said computer file identified as potentially containing malware is prevented from being transmitted outward from a mail server and is further analyzed when being transmitted inward to said mail server.

Rubin does disclose wherein the file identified as potentially containing malware is prevented from being transmitted outward from a mail server and is further analyzed when being transmitted inward to said mail server (page 2 paragraph 3 and page 3 paragraph 3).

Rubin is analogous art because it is directed towards mail protocol virus scanning.

It would have been obvious for one of ordinary skill in the art to modify Kuo and Chen to include the inspection of mail traffic at a mail server for viruses.

Motivation for one to modify Kuo and Chen as discussed above would have been obvious for one of ordinary skill in the art so as to prevent the spread of viruses in Internet mail traffic.

Allowable Subject Matter

Claims 6-7,16-17,26-27, 33 and 35 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Claims 6-7, 16-17, 26-27 and 35 are deemed allowable due to the limitation of specifically adjusting the trigger threshold of a subsequent scan to be more sensitive also by reducing the suspicious activities score required to trigger identification of malware.

Claim 33 is deemed allowable due to the limitation of searching for a target word that is a phonetic equivalent of a target word in the predetermined word library.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon S. Bludau whose telephone number is 571-272-3722. The examiner can normally be reached on Monday -Friday 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Brandon S Bludau
Examiner
Art Unit 2132

BB
***

GILBERTO BARRON Jr.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100